7/15/09

Washington State Health Care Authority
Health Information Infrastructure Advisory Board

Preliminary Report
Privacy and Security Assessments of Health Record Bank Pilots

I. Executive Summary

Privacy and security assessments of the health record bank (HRB) pilots were designed to evaluate the practical implementation issues related to patient control of record access. Criteria were established and material submitted by the pilots was reviewed. Ensuring patient control is difficult, in large part because of the lack of clearly supportive public policy. The pilots are revising their material in response to feedback. Meanwhile, the policy issues regarding patient control should be reviewed by HCA in collaboration with other appropriate stakeholders.

II. Background

Privacy and security are of paramount importance in the handling of personal medical information. Accordingly, a key principle guiding the development and implementation of the health record bank (HRB) pilots is privacy protection through patient control of access to their own information. To be effective, such patient control must occur within a system that provides sufficient security controls to assure that information is only available to authorized personnel.

To evaluate and learn from the real-world implementation of these concepts, the HCA has mandated a privacy and security assessment of each project. To guide this, seven categories of assessment criteria (Appendix) were established after review of several external sources of privacy and security guidance.

III. Procedure

The HRB pilots were asked to submit material relevant to their performance with respect to the assessment criteria. Their initial responses were reviewed and feedback provided. The pilots are now reviewing these comments and considering revisions to their activities and documentation.

IV. Preliminary Results

A. Wenatchee

Two important Exhibits related to "Authorization for Release of Medical Information" from Wenatchee were missing. In the information submitted, the following concerns were noted:

1. agreements for internal personnel with access to data are needed
2. stronger and clearer language is needed in the Registrar agreement
   (e.g. serious penalties for improper use of information)
3. patient control needs to be clearer and more granular

a. "I also am authorizing the Care Team Members to use and/or disclose my health information for treatment (including care coordination), payment, and health care operations (including quality assurance) purposes, even if such uses and disclosures already are allowed or required by law" essentially negates patient control (e.g., since patients have no option to decline TPO disclosure).

b. control choices are limited to: 1) all information available; 2) all except mental health, HIV, and genetic information; or 3) none. This is not sufficient granularity.

c. eliminate "change agreement without notice" [not enforceable]

d. Microsoft HealthVault agreement requires a privacy policy at least as protective as Microsoft's (which is very good); this policy does not appear to meet this requirement

4. Microsoft HealthVault agreement requires a strong information security program in accordance with international standards; it is not clear that this is being done.

5. Copyright of the web site information does not clearly exclude patient data

B. Bellingham

The material submitted was complete. The breach notification policy is thoughtful and reasonably comprehensive and may be useful to the other pilots. Otherwise, similar concerns as for Wenatchee were noted (with the exception of #1, agreements for internal personnel).

C. Spokane

The Spokane HRB is generally compliant with the privacy and security criteria within their own operations. However, patient data is transmitted to GoogleHealth for storage, and no information with respect the privacy and security criteria relative to Google was submitted. Independent review of publicly-available privacy and security information about Google raises serious questions about their compliance with the criteria. While GoogleHealth's privacy policy is generally good, it is confusing because it is subordinate to the overall Google privacy policy (which has several major exceptions to the user's control of their own information). Therefore, users of the Spokane HRB do not have adequate control of their information once it is transferred to Google.

While the Spokane HRB admittedly has minimal influence over GoogleHealth's privacy policies, the lack of clear patient control in that system may be a reason to reconsider its use for HRB purposes. Alternatively, clear public policy with respect to patient control of information in HRBs would address this problem by requiring Google (and all other parties) to ensure the implementation of appropriate measures in this regard.

V. Recommendations

A. Clear, unambiguous, and enforceable law is needed to assure patient control -- this cannot be done easily within existing law

1. HIPAA-covered entities find it difficult to allow patient control

a. Since HIPAA disclosures are not *required*, HIPAA-covered entities could explicitly indicate that they will not make such disclosures

b. Attorneys for HIPAA-covered entities are reluctant to do this

2. non-HIPAA-covered entities may be covered by the Electronic Communications Privacy Act (ECPA) that requires subscriber consent for access

a. but only if their HRB is "publicly available"

b. ECPA is not well known and may not reassure consumers

3. Web privacy policies are enforced by the FTC

a. does not ensure that privacy policies are good

b. FTC enforcement may not sufficiently reassure consumers

B. HCA should facilitate interchange and sharing among the HRB pilots

1. policy discussions
2. exchange of useful documents
3. assistance in identification and application of best practices

VI. Next Steps

A. Pilots will revise and resubmit their materials

B. Final submissions will be reviewed and a subsequent report prepared

C. Policy issues should be considered by HCA (and appropriate stakeholders)

Appendix: Privacy and Security Review Criteria

Security Assessment Criteria:

Principle	**Criteria**	**Comments and additional sources**
A) Authentication of Consumers and other individuals using the system. See Markle CT2 and Christiansen framework (see page 16, "level 3 procedures").	A.1 All users and machines* that interact with the system have been thoroughly authenticated and documented. A.2 Authentication policy is in place and has high level of assurance (see level 3 in Christiansen framework, pg. 16, e.g. identify is vetted against government issued ID.)	Authentication practices form the cornerstone of security and privacy. * Only machines that automatically provide clinical data to the HRB will be authenticated. Users can use any machine with a browser to access the HRB with security code.
B) Binding Agreements are used for all parties and establish a chain of trust. See Christiansen framework (see page 8 on the factors for Business Agreements).	B.1 All agreements are in accordance with the privacy policies and other polices of the system. B.2 Organizations/individuals that serve to register individuals agree to register in accordance with authentication standards. B.3 Consumers execute binding usage agreements. B.4 Providers that access the data execute binding agreements	Evaluate that basic agreements that are used. Use Christiansen (page 8) and Markle frameworks to review the contracts and provide feedback on basic elements contained.
C) Provision with ID and initiation code, out of band. Christiansen framework vaguely identifies this on page 7, "provisioning".	C.1 Users are delivered a user name and code (initial password) to initiate the account. C.2 The information is provided either in person, via US mail or in a manner that can not be intercepted.	Review process flow and basic procedures to ensure elements that lead to non-repudiation are in place and effective. Identify any holes and provide guidance.

Privacy Criteria:

Principle	Criteria (references to PPC)	Comments and additional sources
D) Policy Notice to Consumers. See Markle CP2 and PPC criteria	D.1 Patients have easy access to the written privacy policy and any related materials. (1.3, 1.10, 1.11) D.2 Policy is written in a manner that is easy to understand. (1.4, 1.5, 1.6, 1.7, 1.8, 1.9) D.3 Policy statement explicitly includes all related technology vendors and applies to all "downstream" companies that may have access the information. (1.2, 2.2, 2.6, 2.8, 2.14) D.4 Policy and or related materials clearly describe who and when/how others may have access to the personal information. (1.2, 2.4, 2.6, 2.7, 2.8) D.5 Policy clearly binds other that may have access to the information. (2.14, 4.1, 4.2)	Transparency is a key to trust, policy should be clear, easily accessible and apply to all downstream entities. E) Determining if a policy is "easily understood" is subjective and requires the assessor to provide meaningful feedback and edits so that improvement ideas are actionable, use of PPC specific criteria may be helpful in this regard.
F) Consumer Consent. See Markle CP3 and PPC criteria	F.1 Patients have clearly "opted in" to put their data into the HRB and any related applications. (3.1, 3.2) F.2 Patients clearly consent to the release of their data to specific individuals/organizations and or to role based situations if proper patient consent is communicated and subsequently obtained, including but not limited to any use or sales of the data in aggregate form. (2.8, 3.1, 4.1)	Tell consumers what you will and won't do with their data, disclose all third parties involved. Consumers explicitly decide to be included in all uses of their data, even if in aggregated form.

G) Consumer Obtainment and Control See Markle CP8 and PPC criteria:	G.1 Patients are told what data they can control and any limitations that may exist. (1.1, 2.5, 13.4) G.2 Patients are told how their data may be accessed during an emergency and how such an emergency is later reviewed and they are notified. (7.6, 7.7, 2.6, 2.7, 2.10, 2.11, 10.1) G.3 Patient may choose to close their account and delete all records within a specified time. (3.3, 6.2)	describe accurately to consumers the extent to which the employed technology let's them control who sees what and to what degree of granularity
H) Immutable Audit Trails. See Markle CT3 and PPC criteria.	H.1 Ensure audit trails are in place for all occurrences of data access, batch and real time. (9.1, 9.2, 9.3, 9.4, 9.5) H.2 Can audit trails be produced if requested by the patient? (9.7) H.3 Are audit trails immutable and secure? (9.6) H.4 Patients have ability to report concerns about privacy or security concerns.	Develop audit trails as far as we can towards a log of who-saw-what-info-when
I) Limitations on Identifying Information. See Markle CT4 and PPC criteria:	I.1 Patients are told about profiling or tracking practices and the specific data used for this purpose is disclosed. (5.1, 5.2)	Understand and disclose the extent to which the pilots and their partners will be capturing electronic-not demographic-identifiers and what risks that poses and especially if that information is shared with other organizations.